IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
ST. JOSEPH DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JOSHUA HOWLAND, and RYAN NEAL MONTGOMERY, Defendants.	Case No. 5:20-cr-06007-DGK

UNITED STATES' NOTICE OF EXPERT WITNESSES
PURSUANT TO FEDERAL RULE OF CRIMINAL PROCEDURE 16

The United States of America, through Trial Attorney Kyle Reynolds, and Assistant United States Attorneys David Luna and Alison D. Dunning, submits the following notice pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G) regarding expert testimony. The Government makes no representation that any of the following witnesses are required to be qualified or disclosed as experts or that any portion of their anticipated testimony is in fact expert testimony in the sense contemplated by Fed. R. Crim. P. 16(a)(1)(G) or Fed. R. Evid. 702, *et seq*. Nevertheless, the Government provides the following disclosures out of an abundance of caution.

James Fottrell

Mr. Fottrell is the Director of the High Technology Investigative Unit ("HTIU") at the U.S. Department of Justice, Criminal Division, Child Exploitation and Obscenity Section. He has held this position since 2002, and he has been a computer forensic examiner since 1989. In his capacity of Director of HTIU, Mr. Fottrell supervises a team of Digital Investigative Analysts who conduct forensic analysis of seized computer systems, servers, mobile devices, and other media to provide

investigative and analytical support to prosecutors and law enforcement agents. He regularly conducts online investigations and analysis of internet technologies used to commit federal child exploitation offenses. He has conducted and assisted with numerous investigations involving the Tor network and with child pornography offenses involving the Tor network. He has numerous certifications, including certifications in Encase and computer evidence recovery training. In addition to his on-the-job experience analyzing digital devices, he has taken and taught numerous training courses connected to the analysis of computers and online child exploitation offenses, including offenses on the Tor network. Mr. Fottrell has testified as an expert in numerous federal child exploitation trials on the subject of gathering and assessing digital forensic evidence as well as the investigation of child exploitation crimes on the internet. He holds a bachelor's degree in computer science from the State University of New York, College at Oswego. His curriculum vitae has been provided to the Defendants' counsel.

In the last four years, Mr. Fottrell has testified as an expert witness in the following cases: *United States v. Clint Robert Schram*, 5:20-cr-06002 (W.D. Mo. 2023); *United States v. Christopher Kuehner*, 1:22-cr-00120 (E.D. Va. 2023); *United States v. Derek Flaming*, 4:21-cr-00281 (N.D. Okla. 2022); *United States v. Ashley Kolhoff*, 1:21-cr-00158 (E.D. Va. 2022); *United States v. Joshua Duggar*, 5:21-cr-50014 (W.D. Ark. 2021); *United States v. James Clawson*, 1:20-cr-00119 (E.D. Va. 2021); and *United States v. Christopher Sueiro*, 1:17-cr-00284 (E.D. Va. 2021). Mr. Fottrell testified in *Commonwealth of Massachusetts v. Helmdean Noel*, 2084CR00175 (Superior Court, Suffolk County Criminal 2023). He has authored no publications in the last ten years.

The United States may call Mr. Fottrell to testify about a computer network known as "Tor" (an abbreviation for "The Onion Router"), including its purpose, the way it operates, and difficulties that it poses for criminal investigations. In particular, he may contrast the Tor network with the

"clearnet" or the ordinary internet. Mr. Fottrell may testify that the internet is a global network of computers and other devices that are uniquely identified by internet protocol addresses, also known as "IP addresses." Generally, when one device on the internet requests information from a second device, the requesting device identifies its own IP address and communicates it directly to the responding device so that the responding device knows where to send its response. Data transferred over the internet is split into "packets" that contain two parts: a "header" that contains non-content routing and control information, such as a packet's source and destination IP addresses, and a "payload," which generally contains user data or the content of a communication.

Mr. Fottrell may testify that when individuals commit crimes over the clearnet, law enforcement is frequently available to identify that individual's IP address and then use that information to more specifically identify an offender or a location where the offense took place. For example, if a computer user uses a website to commit a crime, that website frequently records the IP address of the user on a website log. Law enforcement can often then obtain the computer user's IP address from the website, and it can often then determine from an internet service provider the user account that was using that IP address at the time the crime took place. In addition, if a clearnet website itself is facilitating criminal activity, law enforcement can generally determine the IP address of the computer server hosting the website by looking it up on a publicly available Domain Name System ("DNS") listing, which provides information about clearnet websites.

Mr. Fottrell testify that the Tor network is a computer network available to internet users that is designed to facilitate anonymous communication over the internet and to make it more difficult to determine the identity and location of a computer user. The Tor network does this by routing communication through a globally distributed network of relay computers or "nodes," along a randomly assigned path known as a "circuit."

Mr. Fottrell may testify that to access the Tor network, a user must install Tor software, which is most easily done by downloading the free "Tor Browser" from the Tor Project, which is a private entity that maintains the Tor network. The Tor browser is a web browser that is configured to route a user's internet traffic through the Tor network. A user may also access and use the Tor network through any computer or electronic device that has been configured to use Tor routing or software, including desktop or laptop computers, smartphones, or tablet computers.

Mr. Fottrell may further testify that, as with other internet communications, a Tor user's communications are split into packet that contain header information and a payload and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares his or her IP address with Tor nodes. This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers—individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

Mr. Fottrell may testify that Tor may be used to access clearnet websites. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user access such a clearnet website, only the IP address of the last relay computer—known as the "exit node"—appears on that website's IP address web access log. Put differently, the website can see only the IP address of the computer serving as the exit node, not the computer user's actual IP address. Accordingly, unlike over the clearnet, law enforcement generally cannot identify or locate a Tor user who has committed a crime over a website by obtaining an IP address from the website's logs, because that IP address will not be the computer user's true IP address. In addition,

the contents of a Tor user's communications are encrypted while the communication passes through the Tor network, which prevents the operator of a Tor node from observing the content of other Tor users' communications.

Mr. Fottrell may further testify that the Tor network makes it possible for users to operate and access websites that are accessible only to users operating over the Tor network and not users operating over the clearnet only. Such websites that are accessible only over the Tor network are called "hidden services" or "onion services," and they are part of what is sometimes referred to as the "dark web." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. Hidden services, however, have unique technical features that attempt to conceal the computer server's location.

Mr. Fottrell may further testify that, unlike standard internet websites, the web address of a Tor-based hidden service consists of a series of 16 or 56 algorithm-generated characters, followed by the suffix ".onion." Unlike clearnet websites, there is no way to determine the IP address of a computer server that hosts a Tor hidden service through a DNS query. Because of this, while law enforcement can visit, view, and access Tor hidden services that are facilitating illegal activity, they cannot determine the IP address of such a hidden service through public lookups. In addition, as with all Tor communications, communications between Tor users' computers and a Tor hidden service webserver are routed through a series of intermediary computers.

Mr. Fottrell may further testify that numerous websites dedicated to child pornography have operated over the Tor network, and that the nature and operation of the network has made it difficult for law enforcement to determine the location of the website servers, the identity or location of the individuals behind the website, and the identity or location of the website users.

In accordance with Fed. R. Crim. P. 16(a)(1)(G)(v), I approve this disclosure:

JAMES FOTTRELL

Digitally signed by JAMES FOTTRELL
Date: 2023.09.28 15:30:24 -04'00'

James Fottrell

Aaron Butzin

Aaron Butzin is a Lead Software Engineer with the MITRE Corporation. Between June 2014 and September 2023, he was a Special Agent with the Federal Bureau of Investigation. Before joining the MITRE Corporation, he was assigned to the Cyber squad in the FBI's Indianapolis Field Office, investigating criminal computer intrusions. Before joining the Indianapolis office, he was assigned to the Child Exploitation Operational Unit within the FBI's Criminal Investigative Division. As part of the Child Exploitation Operational Unit, Mr. Butzin investigated complex, high-technology criminal offenses involving the sexual abuse and exploitation of children, including child pornography websites and offenders operating over the Tor network.

Mr. Butzin holds a bachelor's degree in computer science from Anderson University. Mr. Butzin also has ten years of private software development experience using a myriad of technologies including Microsoft C#, Microsoft SQL Server, MySQL, python, and ruby in both Windows and Linux environments. After joining the FBI, Mr. Butzin developed custom applications for the bureau using a myriad of technologies including python, MySQL, nginx, and Linux. He testified as an expert witness in *United States v. Clint Robert Schram*, 5:20-cr-06002 (W.D. Mo. 2023). He has not authored any publications in the last ten years.

The United States may call Mr. Butzin at trial to testify that Website A—specified in the Second Superseding Indictment—was being hosted and maintained from the home of Clint Robert Schram in Kansas City, Missouri. Specifically, he may testify that he was present at the search warrant at Mr. Schram's home in Kansas City on July 22, 2020, and during the execution of that

warrant, he encountered an HP Pavilion model 510-P114 desktop computer with serial number CNV63707Q0. Defendant provided the credentials to unlock the computer.

Mr. Butzin used credentials provided by Mr. Schram to unlock this computer, and during his examination of it, he observed that the HP Desktop was running a Linux variant and that two "virtual machines" were active and operating on the computer. A "virtual machine" is a computer system created using software on one physical computer in order to emulate the functionality of another separate physical computer. One of the virtual machines was set up as a "gateway" that served as the other virtual machine's connection to the internet and maintained the connection to the Tor network. The other virtual machine was set up as a "workstation" where the user applications were running. He may further testify that this setup—which is known as Whonix, a virtual machine acting as a gateway, and another virtual machine acting as a workstation—is used to protect the workstation virtual machine from malicious attacks and provide maximum privacy and security for users by making dns leaks impossible and limiting what user applications are able to do.

Mr. Butzin examined the gateway virtual machine and reviewed the contents of a folder located at "/var/lib/tor/." He may testify that this folder contained data used and maintained by the Tor application that is necessary to connect to the Tor network. He may further testify that within the "/var/lib/tor" directory, he located a folder that contained the full name of Website A. This folder contained the necessary files to publish an onion service, including a file named "hostname", which included the onion address (URL) of the website. The contents of the hostname file in this folder corresponded with the URL of Website A. This folder also contained an onion service "encryption key." Onion services provide end-to-end encryption of data sent to and from the service, meaning that communication is encrypted before being transmitted and decrypted upon receipt. The encryption keys are used in that encryption/decryption process.

Mr. Butzin may further testify that he examined the workstation virtual machine and determined that it had "nginx" installed and was configured with a root directory of "/var/www/html." "Nginx" is an open-source web server, an application that stores and delivers the content for a website, such as text, images, video, and application data, to clients that request it. A "root directory", as it relates to nginx, is the location of the files that nginx will deliver when requested. He may further testify that he examined this directory and identified a file ending with the extension ".php." He may testify that a ".php" file contains source code written in the PHP programming language. Source code is human-readable computer instructions written in a programming language, like PHP, that are translated into machine instructions that make up a computer program. This ".php" file was named with the partial name of Website A and contained a customized version of "le_chat_php", the program used to run Website A.

Mr. Butzin may further testify that he located another folder within the workstation virtual machine at the location "/var/lib/mysql." "MySQL" is a relational database management system used to store and retrieve data used by applications like "le_chat_php". This folder contained files necessary for the MySQL application to run and included a subfolder that contained the full name of Website A. This subfolder contained data files related to Website A, and contained the information stored by "le_chat_php" including the list of registered users and their attributes, chat messages, admin notes, and system settings, as well as other data for those websites.

Mr. Butzin may testify that the computer forensic evidence and artifacts discussed above are unique characteristics of computers that are hosting websites and making them available over the internet, including the Tor network, and that the existence of this evidence and artifacts confirms that the HP Desktop computer in Mr. Schram's home was in fact hosting and making available Website A to users over the Tor network. He may further testify about any matter discussed or

implicated in his March 27, 2023, FD-302 report, a copy of which will be provided to the Defendants' counsel contemporaneously with the filing of this notice.

In accordance with Fed. R. Crim. P. 16(a)(1)(G)(v), I approve this disclosure:

Aaron Butzin

Amy Corrigan

Ms. Corrigan is a Digital Forensic Examiner with the Federal Bureau of Investigation (FBI), Kansas City Division, assigned to the Heart of America Regional Computer Forensics Laboratory (HARCFL), and has held this position since March, 2013. Ms. Corrigan has conducted forensic analysis of hundreds of seized computer systems, servers, mobile devices, and other media to provide investigative and analytical support to prosecutors and law enforcement agents. She also assists with and performs on-site search and seizure operations. She regularly uses tools and other investigative techniques to document the contents, physical location, and other identifying information of seized media. She has worked for the FBI since June 2003 with prior assignments as a Program Manager for the Computer Analysis Response Team (CART) Training Program, a Program Manager for the Proficiency Test Program for the Digital Evidence Laboratory (DEL), a Program Manager for the DEL Training Program, and as a Program Manager for the DEL Quality Assurance Program. Before joining the FBI, she worked as a Documentation Analyst for Wetherill Associates, Inc., as a Software Engineer for Aydin Computer and Monitor, as a Software Engineer and a Training Specialist-Software Engineer at General Dynamics, and as an Adjunct Professor in Math and Computer Science at Park College, Carswell Air Force Base. Ms. Corrigan holds a bachelor of science degree with a double major in mathematics and computer science from

Northwest Missouri State University and has completed graduate coursework toward a master's degree in science in computer science. Ms. Corrigan has also completed graduate coursework toward a degree in corporate training and development. Ms. Corrigan has not authored any publications in the previous ten years. In the last four years, Ms. Corrigan has testified as an expert witness in the following cases: *United States v. Shawn Burkhalter, et al.*, 18-00036-01/02-CR-W-BCW, United States District Court, Western District of Missouri (August 2023); *United States v. Anthony Jordan*, 4:15-CR-404-HEA, United States District Court, Eastern District of Missouri (July 2023); *State of Missouri v. Michael Hendricks*, 2116-CR01799-01, and *State of Missouri v. Maggie P. Ybarra*, 2116-CR01768-01, Jackson County Circuit Court (tried jointly) (July 2023); *United States v. Clint Robert Schram*, 20-06002-01-CR-SJ-SRB, United States District Court, Western District of Missouri (May 2023); *State of Missouri v. Eugene Birdsong*, 1816-CR05677, Jackson County Circuit Court (February 2023); *State of Missouri v. Rashidi Crosdale*, 2016-CR02020, Jackson County Circuit Court (February 2023); *State of Missouri v. Tyree West*, 2016-CR02021, Jackson County Circuit Court (February 2023); *United States v. Ladele D. Smith, et. al.,* 19-00315-CR-W-DGK, United States District Court, Western District of Missouri (September 2022); *State of Missouri v. Brian Keeling*, 21AE-CR03074-01, Platte County Circuit Court (August 2022); *United States v. Kevin Lewis*, 6:20-CR-10028-EFM-11, United States District Court, District of Kansas (March 2022); *State of Missouri v. Damon Kerr*, 1916-CR00647-01, Jackson County Circuit Court (March 2022); *State of Missouri v. Tanner Johnson*, 19LV-CR00334-01, Livingston County Circuit Court (July 2021); *State of Kansas v. Grant Nixon*, 2019-CR-000186, Leavenworth County District Court (October 2019); *United States v. Ebube Otuonye*, 6:18-CR-10085-EFM-1, United States District Court, District of Kansas (July 2019). A copy of Ms. Corrigan's updated curriculum vitae will be provided to defense counsel contemporaneously with this notice.

The Government may call Ms. Corrigan to testify on matters concerning the computer forensic analysis of computers and other digital devices seized from the search of defendant Ryan Neal Montgomery's home on October 28, 2020, and computers and digital devices seized from the search of defendant Joshua Howland's home on October 7, 2020. She may testify that she assisted with the forensic imaging of devices seized from Montgomery's and Howland's homes and that the forensic images created of those devices are authentic and reliable. Ms. Corrigan may further testify that she conducted a computer forensic analysis of certain digital devices seized from Montgomery's home, including an IBM 1GB Microdrive compact flash card recovered from a gray Canon Powershot G1 PC1004 digital camera with serial number 182D00558 (Item 1B40), a large silver iPad A1876 with serial number DLXXR2U8K7MC (Item 1B36), a black HP 15-ax-243dx laptop with serial number 5CD70713KR containing a Crucial FCCT960M500SSD1 960GB SATA hard drive with serial number 133209492E32 and a Samsung 860 EVO 1TB M.2 drive with serial number S415NB0KB07229R (Item 1B41), and black Google G011A Pixel 2 cell phone with IMEI (on tray) 357537082472317 (Item 1B37). Ms. Corrigan may further testify that she conducted a computer forensic analysis of certain digital devices seized from Howland's home, including a Google Pixel 4A with IMEI (from settings) 357511100925069(1) and 357511100925077(2) (Item 1B42), and a Google Pixel 3 64GB with IMEI 990012001523593 (Item 1B43). Ms. Corrigan may testify that she used standard and reliable forensic tools, including AccessData Lab (AD Lab), Internet Evidence Finder (IEF) (now Axiom), FTK Imager, Cellebrite UFED4PC, and Cellebrite UFED Physical Analyzer, to analyze the file structure of these devices, analyze applications on the devices, and mount them to view their contents.

Regarding defendant Montgomery's devices, Ms. Corrigan may testify that she mounted a forensic image of the HP laptop (Item 1B41), and was able to identify information that included a

large amount of child exploitation activity, use of the Tor browser, a large number of chat logs from Website A, artifacts showing the use of IP address 73.157.250.255, non-pornographic photographs of young-appearing girls, and evidence of use of the HP laptop by Montgomery. Ms. Corrigan may further testify that she mounted a forensic image of the large silver iPad (Item 1B36) and was able to identify information indicative of a history of browsing child pornography websites.

Ms. Corrigan may testify that she conducted analysis on the black HP laptop (Item 1B41) and found over 47,000 images and videos of child pornography (CP) (also referred to as child sexual abuse material (CSAM)), and child exploitive (child erotica) or age indeterminate material. Of those, approximately 1,514 were CP/CSAM images and videos depicting known and unknown infant or toddler-aged victims (with approximately 33 of those images/videos depicting bondage or violence) and approximately 7,093 were CP/CSAM images and videos depicting known and unknown prepubescent victims (with approximately 117 of those images/videos depicting bondage or violence). Ms. Corrigan may testify that a large amount of child exploitive (child erotica) or age indeterminate material was also located. Of those, approximately 859 images and videos depicted infant or toddler-aged victims (with approximately 534 of those images/videos depicting bondage or violence). The remaining approximately 36,000 images and videos were categorized as "other" depicting known and unknown victims, a small number of which depicted bondage or violence.

Ms. Corrigan may also testify that in addition to these images and videos, which were identified by hash value, many other images and videos of children in sexual or erotic poses were located on the HP laptop's two hard drives (Item 1B41). On the Samsung 860 EVO 1TB M.2 drive with serial number S415NB0KB07229R, all of the above-described items came from a folder called "Etc." On the Crucial FCCT960M500SSD1 960GB SATA hard drive with serial number 133209492E32, all of the above-described items came from the Desktop, Documents and

Downloads folders for the user account "Ryan." Ms. Corrigan may also testify that other 400,000 additional files were contained in these folders and many of those, although not all, are possible child pornography or child exploitive (child erotica) material. Ms. Corrigan may also testify regarding the identification of and the process of identifying images and videos as possible child pornography as well as the meaning and usage of certain terms and phrases typically associated with child pornography.

Ms. Corrigan may also testify that she located over 400 files containing chat logs for Website A, including user account nicknames and discussion comments, with creation dates from August 14, 2019 to July 3, 2020. Most of the logs were in the Downloads folder for user "Ryan," but 15 logs had been saved on the Samsung 1TB hard drive in Montgomery's HP laptop. Ms. Corrigan may testify that she located a chat from March 11, 2020 that contained text mentioned in the search warrant affidavit.

Ms. Corrigan may testify that the Tor browser was installed on Montgomery's HP laptop (Item 1B41), and that settings for the Tor browser were such that some bookmarks and autofill entries were saved. Ms. Corrigan may testify about Firefox activity related to Website A and Firefox activity related to all dark web (.onion) sites. Firefox history was located showing visits to several dark web sites, including Website A (including showing access for Montgomery's username on Website A) and other sites with names indicating a focus on child exploitation. Ms. Corrigan may also testify that dark web bookmarks for Website A and other sites indicating a focus on child exploitation were saved for the timeframe between March 25, 2019 and September 5, 2020. An autofill entry for the field "nick" (possibly an abbreviation for nickname) had the value of Montgomery's username on Website A, and was first used July 23, 2019 and last used July 22, 2020. An autofill entry for the file "req_username" had the value of Montgomery's username on Website

A, and was first used on August 2, 2020 and was last used on October 21, 2020. Additionally, Ms. Corrigan may testify that hundreds of autofill entries for a field called "message" were located in Firefox Form History. These entries appear to be moderator comments and show only messages issued from the HP laptop. Ms. Corrigan may testify that one of the entries corresponds to a reference in the search warrant affidavit.

Ms. Corrigan may testify regarding the location on the HP laptop (Item 1B41) of artifacts of interest in connection with a file of interest, "heartstrings.7z," mentioned in the search warrant affidavit. A file called "heartstrings.7z" containing files like "follow1.JPG" was accessed on June 1, 2020 at 00:51:44. A Firefox Form History "message" field entry corresponds to a reference in the search warrant regarding a file downloaded on June 21, 2020. Additionally, a jumplist artifact was located showing the file "follow1.JPG" was opened in Photos Microsoft (Windows 10) just a few minutes later. Ms. Corrigan may further testify that the "heartstrings.7z" file and "follow1.JPG" are no longer on the HP laptop hard drives.

Ms. Corrigan may testify that Montgomery's HP laptop (Item 1B41) contained a folder with non-pornographic photographs of young appearing girls that were taken with a Google Pixel 2 cell phone. Some of the pictures appeared to be taken in-person, and others appeared to be photographs of posters depicting girls.

Ms. Corrigan may testify that she located items indicative of ownership or primary use of the HP laptop (Item 1B41) by Ryan Montgomery including a primary user account, "Ryan," plus invoices, photos taken by a Google Pixel 2 cell phone that depicted Montgomery, and emails to and from Montgomery. Ms. Corrigan may also testify about the multiple accounts located on the HP laptop and the IBM 1GB Microdrive compact flash card from the Gray Canon Powershot G1 PC1004 digital camera with serial number 182D00558 (Item 1B40), including, among others, those

containing Montgomery's username on Website A (used 499 times in Firefox—possibly Tor browser—from July 23, 2019 to July 22, 2020) in addition to account names that included all or part of Montgomery's first and/or last names.

Ms. Corrigan may also testify regarding items located on Montgomery's black Google G011A Pixel 2 cell phone with IMEI (on tray) 357537082472317 (Item 1B37). Ms. Corrigan may testify that a search for the term "teen meat" on June 15, 2020 was visible in Autofill. Downloads from 4chan.org throughout 2018 were located that consisted mostly of adult pornography but included videos of females of indeterminate age. A web visit on January 5, 2018 to a Tor .onion URL directory was located in addition to web bookmarks for boards with names indicative of possible child pornography. Ms. Corrigan may also testify that multiple accounts were located including, among others, those that contained all or part of Montgomery's first and/or last names, plus multiple accounts with the same or similar names as those contained in the HP laptop (Item 1B41).

Regarding defendant Howland's devices, Ms. Corrigan may testify regarding items located on the Google Pixel 4A with IMEI (from settings) 357511100925069(1) and 357511100925077(2) (Item 1B42). Ms. Corrigan may testify that the phone contained a folder titled "Girls," which had photographs of naked girls, some of whom had red hair. Some of the images are possible CP/CSAM. Ms. Corrigan may testify that possible CP/CSAM was also located in file paths indicative of being edited with an app called "PicSay." Additionally, videos with filenames indicating they had been trimmed in a video app were located. These videos depicted a girl in a shower and were possible CP/CSAM. Ms. Corrigan may also testify about accounts names noted on the Google Pixel 4A, including among others, those that included all or part of Howland's first and/or last names, in

addition to "GapeHerAss," "MotionlessWhiteGirl," "RapeHerAss," "vermontkindbud," and "WannaB_UrDaddy."

Ms. Corrigan may testify regarding items located in the Google Pixel 3 64GB with IMEI 990012001523593 (Item 1B43). Ms. Corrigan may testify that several images of possible CP/CSAM were located. These were located in file paths indicating they were from videos played in the VideoLAN (VLC) video app and the PicSayPro photo editing app. Ms. Corrigan may also testify that the following accounts were located on the device: "1-802-488-4210," "Joshua Howland," and "vermontkindbud@gmail.com."

Ms. Corrigan may further testify that all the resulting exhibits produced by means of the processes described above are accurate and authentic because of the reliability of the forensic tools and processes used to recover them, internal characteristics that attest to their authenticity, the absence of errors or indications that the processes and tools functioned improperly, and the reliability and durability of electronic data. Ms. Corrigan may further testify as to any matter discussed or implicated in her Reports of Examination dated January 6, 2021, September 13, 2022, May 26, 2023, and September 25, 2023.

In accordance with Fed. R. Crim. P. 16(a)(1)(G)(v), I approve this disclosure:

Amy Corrigan

James McMillian

James McMillian is a police detective with the Olathe, Kansas Police Department. He has been employed as an Olathe Police Officer since May 1999. From January 2019 to the present, Detective McMillian has been assigned as a Digital Forensic Examiner and Federal Bureau of

Investigations (FBI) Task Force Officer with the FBI Computer Analysis Response Team (CART) at the Heart of America Regional Computer Forensics Laboratory (HARCFL). In that capacity, Detective McMillian has conducted forensic extractions and analysis of numerous seized computer systems, mobile devices, and other media to provide investigative and analytical support to prosecutors and law enforcement agents. He regularly uses tools and other investigative techniques to document the contents, physical location, and other identifying information on seized media. Detective McMillian has several certifications relevant to his position as a digital forensic examiner to include FBI CART Technician/Digital Extraction Technician Certification, FBI CART Mobile Device Certification, and FBI CART Forensic Examiner Certification. In addition to his on-the-job experience conducting forensic examinations on digital devices, he has taken numerous training courses connected to the extraction and analysis of computers. His formal training relevant to child exploitation investigations includes child physical and sexual abuse investigative courses as well as child pornography investigative courses. Additionally, Detective McMillian investigated Internet crimes against children, child pornography related crimes, and physical and sexual offenses against children as an Olathe Police detective.

Detective McMillian has not authored any publications in the previous ten years. Detective McMillian testified in May 2022 on the subject of accessing and analyzing digital forensic evidence in a criminal case in *State of Kansas v. Clyde Barnes*, Johnson County Case No. 20CR01599.

Detective McMillian holds a Bachelor of Science in Criminal Justice Administration and an Associate of Science in Law Enforcement from Missouri Southern State University in Joplin, Missouri. Detective McMillian also holds an Associate of Arts in General Studies from Missouri State University in Springfield, Missouri. Detective McMillian's curriculum vitae is provided contemporaneously with this expert notice.

The Government may call Detective McMillian to testify on matters concerning the forensic extraction and analysis of computers, hard drives, and other digital devices both generally and specifically with regard to devices relevant to the instant case. The Government anticipates that Detective McMillian may testify that he imaged, extracted, and analyzed digital devices seized from defendant Joshua Howland during the search of Howland's residence on October 7, 2020. Detective McMillian may testify that he used standard and reliable forensic tools, including AccessData Lab (AD Lab), Internet Evidence Finder (IEF) (now Axiom), and FTK Imager to view, analyze, and report the contents of those devices. Detective McMillian's examination and analysis of Howland's devices located suspected child pornography videos and still images, videos and still images apparently produced by a hidden camera, relevant Internet and TOR usage history, evidence of local files accessed, indicia of ownership of the devices, and the presence of anti-forensic tools. Detective McMillian prepared a Report of Examination dated January 28, 2021 detailing his findings which was reviewed, approved and signed in accordance with HARCFL protocol by his then training supervisor, Forensic Examiner Marcus Fizer.

Specifically, Detective McMillian may testify that he imaged and forensically extracted and examined the contents of a Custom Built ABS Essential Meteor desktop computer (Item HARCFL127084); a Samsung 960 EVO 1 TB M.2 NVMe SSD hard drive, serial number S3X3NF0K501750W (Item HARCFL109819 from Item HARCFL127084); a Teamgroup L5 3D LITE 240 GB SSD hard drive, serial number AA2318161486 (Item HARCFL109820 from Item HARCFL127084); a Seagate Barracuda ST1000DM010 1 TB HDD hard drive, serial number Z9APOQPE (Item HARCFL109821 from Item HARCFL127084); a Seagate 2 TB portable hard drive, serial number NA98SAWT (Item HARCFL127074); a black USB charging block/spy camera (Item HARCFL127072); a Samsung EVO Select 32 GB micro SD card, serial number

KNGDHGSAG942 (Item HARCFL109815 from Item HARCFL127072); a Lenovo Legion Y545 laptop, serial number PF1DY3UA (Item HARCFL127082); A Seagate 1 TB Barracuda Sata hard drive, serial number WN90V9N3 (Item HARCFL109817 from Item HARCFL127082); and a Western Digital PC SN520 PCIe hard drive, serial number 19251A801502 (Item HARCFL109818 from Item HARCFL127082).

It is anticipated that Detective McMillian will testify that upon his forensic analysis of Howland's Samsung 960 EVO 1TB hard drive and Seagate 2 TB hard drive, Detective McMillian located numerous still images and video recordings apparently produced by a hidden camera in a residential bathroom. Many of these images and videos depict females in various stages of undress as they disrobe. Multiple images and videos depict the subjects partially and fully nude and capture the subjects' exposed breasts and genitals. One of the nude subjects of these photos and videos is similar in appearance to an individual known to Howland, and whose identity is known to law enforcement (Victim 1), and is consistent in appearance to a photo of a driver's license of Victim 1 which was located in Howland's Teamgroup L5 3D LITE hard drive. Time stamps on some of the photos and videos of Victim 1 indicate that Victim 1 was under the age of 18 at the time the images and videos were produced. The names of some of these located image and video files indicate their pornographic content. Detective McMillian may testify that forensic analysis located at least approximately 234 additional still image files and at least 28 video files containing child pornography on the Seagate 2 TB hard drive unrelated to and distinguishable from the files produced by an apparent hidden camera referenced above.

Detective McMillian may testify that forensic analysis of the Samsung 960 EVO 1 TB hard drive and the Western Digital PC SN520 PCLE 512 GB hard drive located the Internet and TOR browser history of those devices indicating that the user accessed numerous websites with names

indicative of child pornography related content. Detective McMillian may testify that analysis of the Teamgroup L5 3D LITE 240 GB hard drive located evidence of access to files related to or referencing the name Website A, which is the subject of Counts 1 and 2 of the Indictment. Detective McMillian may testify whether or not images posted by Howland on Website A were visually similar to images located on the devices seized from Howland. Detective McMillian may also testify regarding the identification of and the process of identifying images and videos as possible child pornography as well as the meaning and usage of certain terms and phrases typically associated with child pornography.

Detective McMillian may further testify that all the exhibits resulting from his analysis of the devices described above are accurate and authentic because of the reliability of the forensic tools and processes used to recover them, internal characteristics that attest to their authenticity, the absence of errors or indications that the processes and tools functioned improperly, and the reliability and durability of electronic data. Detective McMillian may further testify as to any matter discussed or implicated in his Report of Examination dated January 28, 2021 previously provided to Howland, as well as any matter referenced in the digital derivative evidence report number HAR-20-516 to which Howland has previously been provided access.

In accordance with Fed. R. Crim. P. 16(a)(1)(G)(v), I approve this disclosure:

James McMillian

Without any further notice or objection by the defense, this filing satisfies the government's obligations under Rule 16(a) in providing a written summary of any testimony that the government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence and applicable court

orders. *See* Fed. R. Crim. P. 16(a)(1)(G). The United States requests reciprocal discovery to the fullest extent of the law, including notice of defense experts under Fed. R. Crim. P. 16(b)(1)(C).

Respectfully submitted,

Steven J. Grocki
Chief, Child Exploitation and Obscenity Section
U.S. Department of Justice, Criminal Division

By: */s/ Kyle Reynolds*

Kyle P. Reynolds
Trial Attorney
Authorized to practice under L.R. 83.5(i)
1301 New York Avenue, NW
Washington, DC 20005
Tel: (202) 616-2842
Fax: (202) 514-1793
Kyle.Reynolds@usdoj.gov

Alison D. Dunning
David Luna
Assistant United States Attorneys
Charles Evans Whittaker Courthouse
400 East Ninth Street, Suite 5510
Kansas City, Missouri 64106
Telephone: (816) 426-4289
Telefax: (816) 426-4322

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing was delivered on September 28, 2023, to the CM-ECF system of the United States District Court for the Western District of Missouri for electronic delivery to all counsel of record.

/s/ Kyle Reynolds
Kyle P. Reynolds
Trial Attorney
U.S. Department of Justice, Criminal Division